8e6 Technologies

8e6® Threat Analysis Reporter

EVALUATION GUIDE

Models: TAR HL/SL/MSA

Software Version: 1.3.00

Document Version: 01.05.09

Downloaded from www.Manualslib.com manuals search engine

THREAT ANALYSIS REPORTER EVALUATION GUIDE

© 2009 8e6 Technologies

All rights reserved. Printed in the United States of America

Local: 714.282.6111 • Domestic U.S.: 1.888.786.7999 • International: +1.714.282.6111

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Downloaded from www.Manualslib.com manuals search engine

CONTENTS

THREAT ANALYSIS REPORTER EVALUATION GUIDE 1

Overview. 1

Note to Evaluators. 1

Install, Configure, and Test TAR. 1

CHAPTER 1: ACCESS THE TAR WEB CLIENT 2

Step 1: Launch IE. 2

Step 2: Type in the URL. 2

Step 3: Log into the Application. 2

CHAPTER 2: DRILL DOWN INTO A URL GAUGE 4

Step 1: How to Read a Gauge. 4

Gauge Name 4

Score 4

Time Span 5

Threat Level 5

Step 2: View Child Gauges. 5

Step 3: View a List of Users Affecting a Child Gauge. 6

Step 4: View an Individual User's Gauge Activity. 6

Step 5: Take Action on an Individual's Activity. 7

Step 6: View Category Details 7

Step 7: View the Actual Web Page Visited by the User. 8

CHAPTER 3: CREATE A NEW URL GAUGE 9

Step 1: Select the Gauges Menu Item. 9

Step 2: Add a Gauge Group. 9

Step 3: Define the Gauge 10

Step 4: Advanced Settings. 11

CHAPTER 4: CREATE AN AUTOMATED ALERT 12

Step 1: Select Alerts. 12

Step 2: Add a New Alert 12

Step 3: Specify Alert Components. 13

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 5: VIEW A URL TREND REPORT 14

Step 1: Access Trend Charts. 14

Step 2: Change the Time Span. 14

CHAPTER 6: MONITOR BANDWIDTH GAUGES 15

Step 1: Select Bandwidth and Outbound..... 15

Step 2: Select the FTP Protocol Gauge..... 15

Step 3: Select Port 21 Child Gauge. 16

Step 4: View the User Summary. 16

Step 5: View Port Traffic..... 17

CHAPTER 7: VIEW A BANDWIDTH TREND REPORT 18

Step 1: Select Bandwidth and Trend Chart. 18

Step 2: View Bandwidth Trend Chart Data. 18

Downloaded from www.Manualslib.com manuals search engine

THREAT ANALYSIS REPORTER EVALUATION GUIDE

Overview

The Threat Analysis Reporter helps administrators manage internal Web-based threats by monitoring Internet usage information by user *in real-time*, and by providing proactive remediation tools to enforce the organization's Acceptable Use Policy.

Note to Evaluators

Thank you for taking the time to review 8e6's Threat Analysis Reporter (TAR) appliance. Your interest in our company and product is greatly appreciated.

This Evaluation Guide Is designed to provide product evaluators an efficient way to install, configure and exercise the main product features of the TAR.

Install, Configure, and Test TAR

To install the TAR appliance, configure the server, and to test the unit to ensure that reporting is operational, please refer to the step-by-step instructions in the Threat Analysis Reporter Quick Start Guide provided inside the carton containing the chassis.

Please note that prior to reviewing TAR, the R3000 Internet Filter must already be installed; this appliance is required for sending logs to the Reporter. See the R3000 Internet Filter Evaluation Guide for instructions on how to set up the Internet Filter.

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 1: ACCESS THE TAR WEB CLIENT

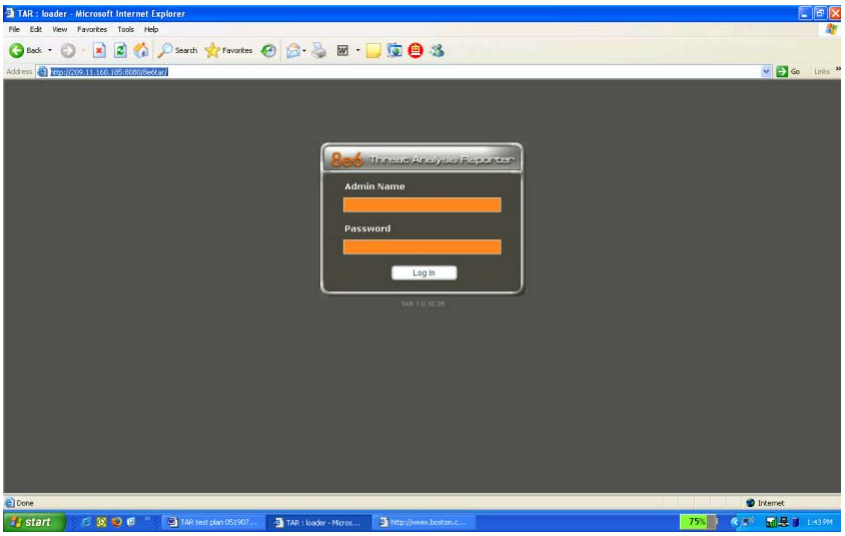
Step 1: Launch IE

From your workstation, launch Internet Explorer to open an IE browser window.

***NOTE**: If pop-up blocking software is installed on the workstation, it must be disabled. Information about disabling pop-up blocking software can be found in the TAR User Guide Appendix A: Disable Pop-up Blocking Software.*

Step 2: Type in the URL

In the Address field of the browser window, type in the URL for the TAR server: **http://x.x.x.x:8080** (in which 'x.x.x.x' represents the IP address). This action opens the TAR login window, which serves as a portal for administrators to log into TAR.



Login window

Step 3: Log into the Application

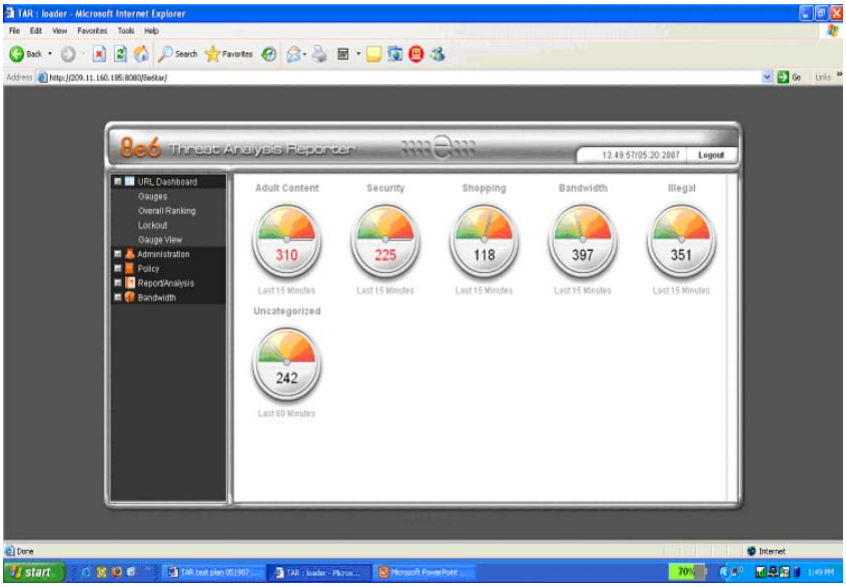
1. In the Username field, type in your username. If you are logging in as the global administrator, enter the username registered during the quick start wizard procedures.

   If you are logging in as a group administrator, enter the username set up for you by the global administrator.

2. In the Password field, type in your password. If you are logging in as the global administrator, enter the password registered during the quick start wizard procedures. If you are logging in as a group administrator, enter the password set up for you by the global administrator. Asterisks display for each character entered.

3. Click the Log In button to open the application that displays the URL dashboard gauge view in the right panel by default. The navigation panel displays to the left, and in the panel above the system time and date display (in the HH:MM:SS/MM.DD.YYYY format) beside the Logout button:

Downloaded from www.Manualslib.com manuals search engine



URL dashboard with URL gauges

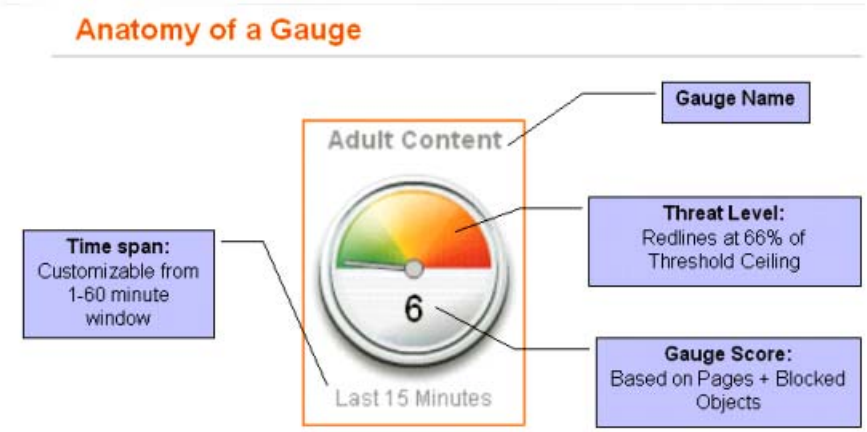
Downloaded from www.Manualslib.com manuals search engine

CHAPTER 2: DRILL DOWN INTO A URL GAUGE

This section will step you through the manual monitoring of users in real-time via the URL gauge dashboard. Note that this is simply one of many ways to use TAR to monitor insider threats. There is also a robust automated alert component that does not require the system administrator to be monitoring gauges in order to be notified of a violation in process.

Step 1: How to Read a Gauge

The graphic below describes how to read gauges on the URL dashboard:



Anatomy of a gauge diagram

Gauge Name

The gauge name is the customized name of the gauge created by the administrator. TAR has five default sample gauges that correspond with five of 8e6's super-categories: Adult Content, Security, Shopping, Bandwidth and Illegal. Administrators can create their own gauges as well as delete the default gauges.

Score

The score is the large number in the center of the gauge that is based upon the number of URL page hits (see NOTE below) that occur in this specific category in a given period of time.

***NOTES**: In addition to page hits, TAR also counts "blocked object" hits. For reference, "pages hits" are files that typically end in .html and represent a main page view. "Object hits" are files that typically end in .gif or .jpg and represent image files.*

To streamline your task, TAR does not track a score for "non-blocked objects," since these gauges are designed to provide a clear picture of how many times a user has requested a page, and objects are images hosted within a page. TAR includes blocked object data to cover instances in which harmful images are hosted on a non-harmful site.

Downloaded from www.Manualslib.com manuals search engine

Time Span

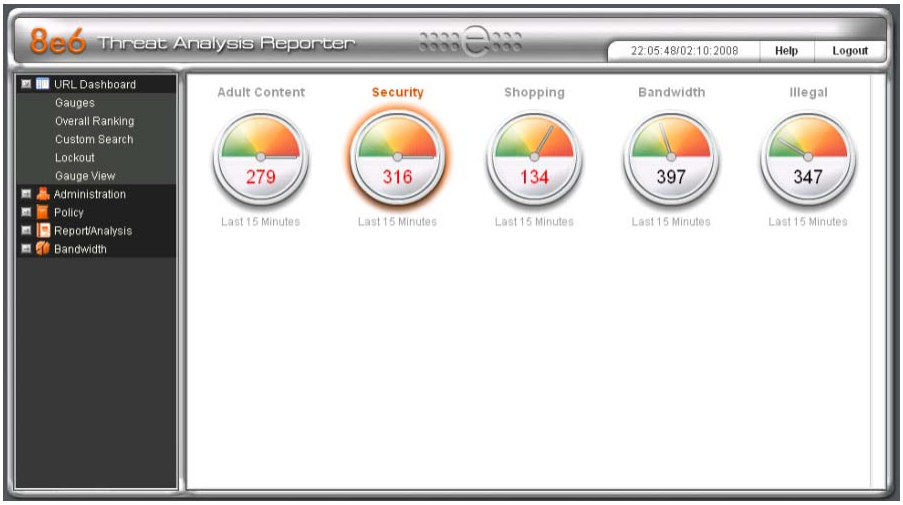
Each gauge monitors events in real-time for a window of time between one and 60 minutes. This time span is customizable by the administrator. For example, if a gauge is set for 15 minutes, that gauge will indicate the number of page hits for the last 15 minutes of time. For example, if the current time is 12:00, the gauge score will reflect all activity from 11:45 to 12:00. Once the time is 12:01, the gauge will reflect all activity from 11:46 to 12:01.

Threat Level

The colored threat level indicates the current state of threat based on the customizable ceiling created by the administrator. For example, if the administrator creates a gauge with a threshold of 100, when the score reaches 67 the gauge dial will move into the red section of the dial and the score number will turn red and begin to flash. These gauges are designed to provide an intuitive reminder when a specific category gauge is experiencing abnormal levels of activity so the administrator can react quickly.

Step 2: View Child Gauges

Sometimes a single child gauge is responsible for driving a parent gauge's score. To view child gauges, you can either double-click the parent gauge or right-click the parent gauge and then select "View Gauge Details". In this example, select the "Security" gauge.



Select the Security parent gauge

Performing either of the two aforementioned actions on this parent gauge will open a window containing all child gauges associated with that gauge.

Downloaded from www.Manualslib.com manuals search engine

Step 3: View a List of Users Affecting a Child Gauge

Double-click the child gauge to open a window containing a list of users who are responsible for driving that gauge's score. In this example, double-click the "Spyware" child gauge.

Open the child gauges window

Step 4: View an Individual User's Gauge Activity

In the Spyware window, select the top name from the user list and click "User Summary" to get a complete view of all activity for that user. This will help determine if the user is just abusing a single category or has high activity in other gauges as well.

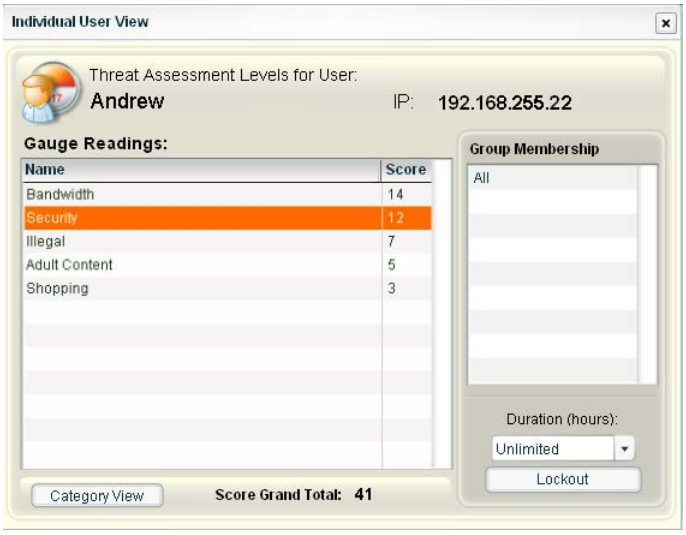
View a list of end users who are responsible for a gauge's activity

Downloaded from www.Manualslib.com manuals search engine

Step 5: Take Action on an Individual's Activity

In the Individual User View window, select the "Security" gauge from the list and then click the "Category View" button to view the hits and score the user obtained for each Security sub-category.

The Individual User View window also lets you lock out the user from further accessing a category. This action is called a "manual lockout." Lockouts can be defined from 30 minutes to eight hours or set for an unlimited amount of time until the administrator manually unlocks the user.

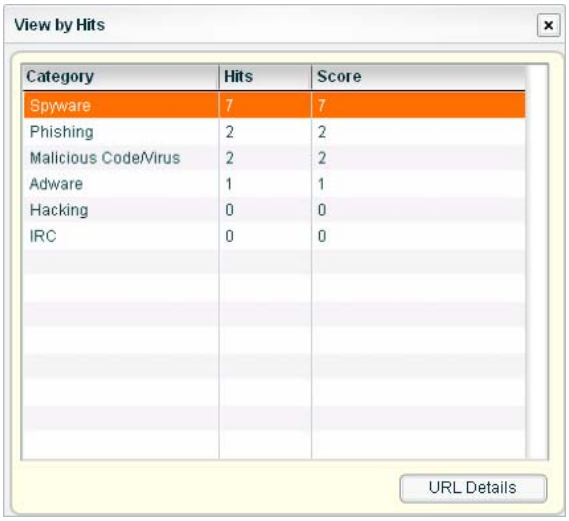


View a summary of an end user's activity

***NOTE**: There is also a way to automatically lock out the user that will be demonstrated later in this document.*

Step 6: View Category Details

In the View by Hits window for the Security category, select the "Spyware" sub-category and then click the "URL Details" button to drill down into the actual pages visited by this specific user in this specific category.

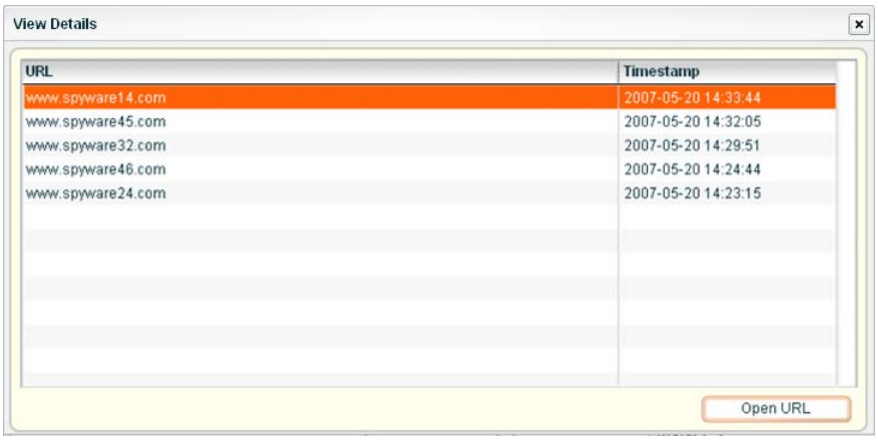


View a list of sub-categories

Downloaded from www.Manualslib.com manuals search engine

Step 7: View the Actual Web Page Visited by the User

You can now view the full URL details for this specific user. In this example, select the first URL in the list and then click “Open URL” to open the actual Web page the end user visited.



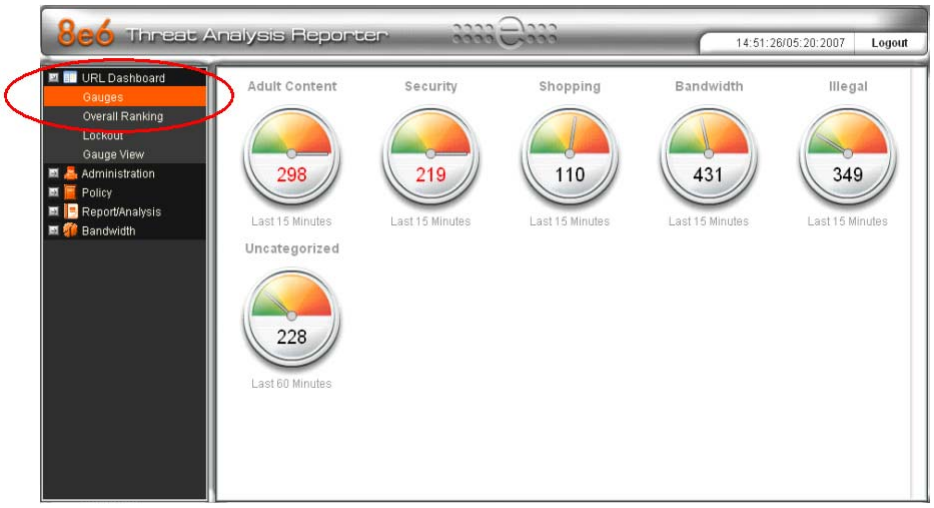
View URL Details

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 3: CREATE A NEW URL GAUGE

Step 1: Select the Gauges Menu Item

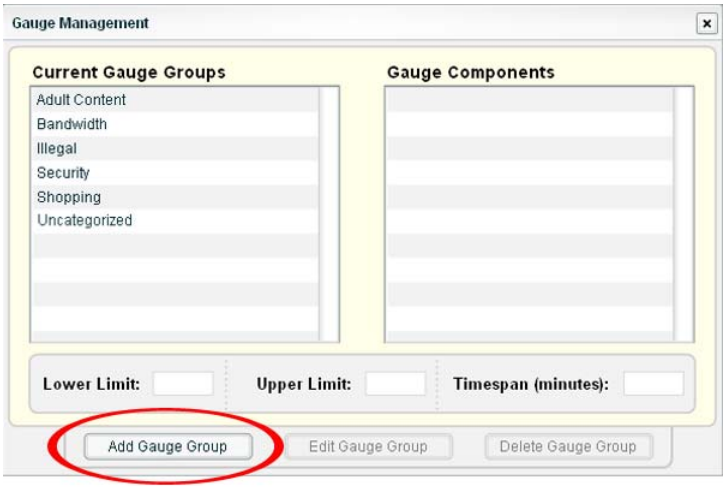
In order to create a new custom gauge, select the “Gauges” menu item from the left-hand menu. This action will open a pop-up window (see Step 2).



Select Gauges from left panel

Step 2: Add a Gauge Group

Click on the “Add Gauge Group” button to set parameters for the gauge.

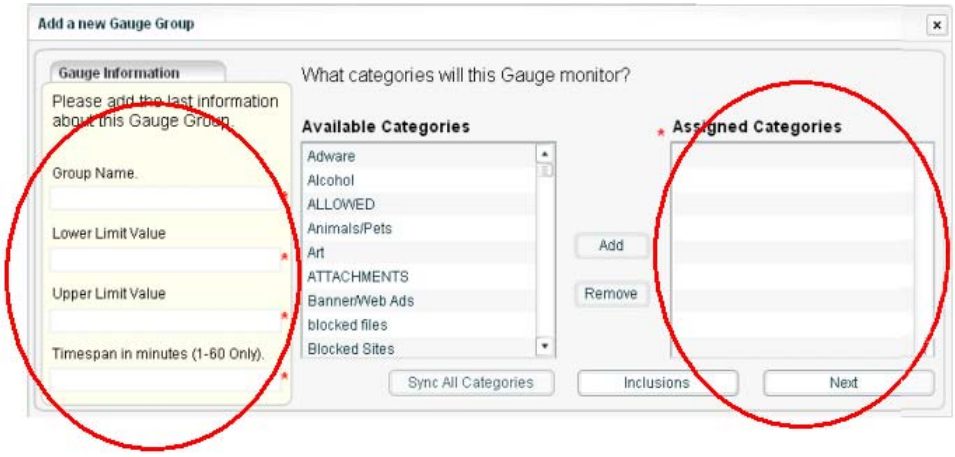


Add a new gauge

Downloaded from www.Manualslib.com manuals search engine

Step 3: Define the Gauge

This section will explain how to set parameters for the new custom gauge.



Define components for the gauge

1. Type in a name in the “Group Name” field (name it whatever you like).
2. Put in ‘0’ in the “Lower Limit Value” field.
3. Put in ‘1000’ in the “Upper Limit Value” field.

***NOTE**: If you do not know what number to set for the upper limit threshold, you can get a better idea by running a URL Trend Report for “One Day” to see the normal level of activity for that category and then set the threshold slightly above that level. See Chapter 5: View a URL Trend Report for details on how to use the trend report.*

4. Put ’60’ in the “Timespan” field.
5. Add “Adware”, “Alcohol” and “Art” into the “Assigned Categories” field by selecting each category and then clicking the “Add” button.

***TIP**: If you make a mistake, just click on the category you do not want and click the “Remove” button.*

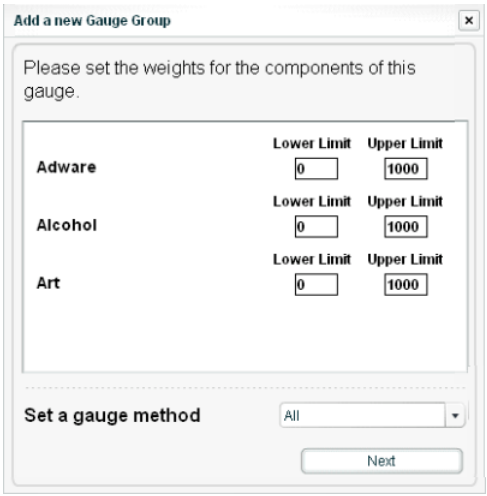
6. Once all of this is completed, click the “Next” button.

***NOTE**: The “Inclusions” button is used to view a subset of users such as the marketing department or classroom 5A. For the sake of this demo, do not change the inclusions default of “All” users.*

Downloaded from www.Manualslib.com manuals search engine

Step 4: Advanced Settings

For the purposes of this demonstration, click the “Next” button to open a window where you configure advanced settings.



Specify thresholds and the gauge method

In this window you can specify different thresholds for each child category. For example, if you deemed “Alcohol” more critical than “Art” you would set a lower threshold for Alcohol. Also, you can choose a different gauge method other than “All”. For example, you might select a gauge method that only monitors Keywords, though a change at this field is not required.

Once you click “Next”, the gauge setup wizard closes and takes you back to the dashboard where your new gauge will begin to show traffic.

***NOTE**: The initial gauge setup may take a few minutes. Once setup is complete, the gauge will report data in real-time.*

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 4: CREATE AN AUTOMATED ALERT

This section will step you through the process of creating an automated threshold per user, so you can be automatically notified via email and the violating user will be automatically locked out once a threshold is exceeded.

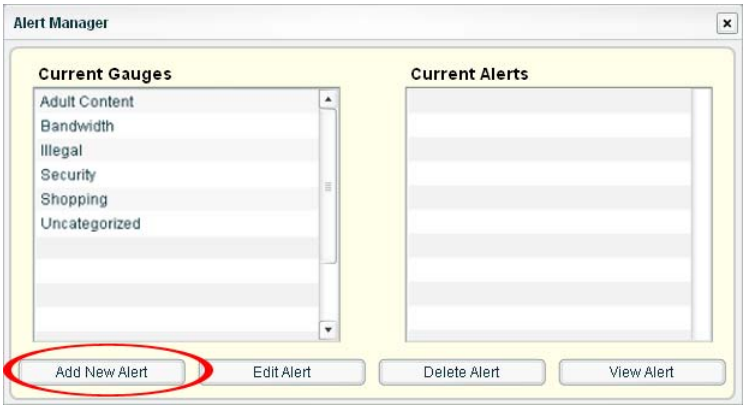
Step 1: Select Alerts

In the left-hand menu tree, click “Policy” to explode the sub-options, and then click “Alerts”. This action will open a pop-up window (see Step 2).

Select Alerts from left panel

Step 2: Add a New Alert

Click on the “Add New Alert” button to set parameters for the alert.



Add a new alert

Downloaded from www.Manualslib.com manuals search engine

Step 3: Specify Alert Components

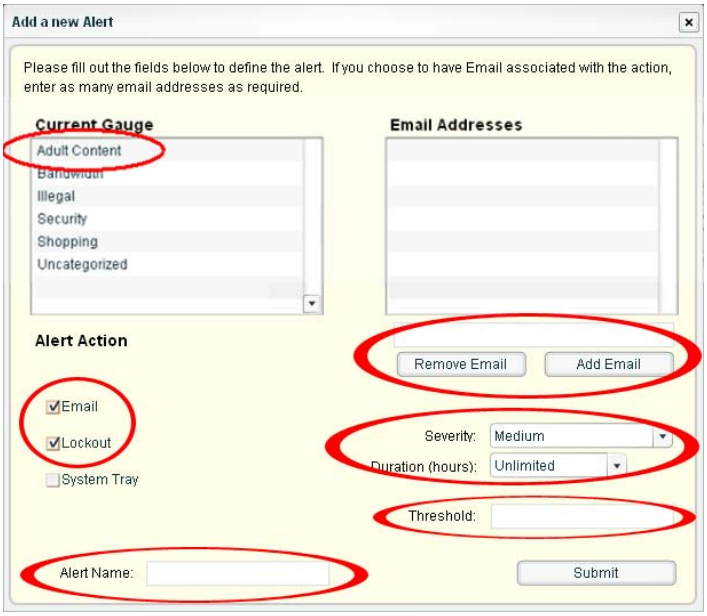
Create a new alert by performing the following actions:

1. Click on one of the gauge names in the “Current Gauge” list (e.g. “Adult Content”).
2. Enable Alert Action checkboxes for “Email” and “Lockout”.
3. Type in the name for your alert in the “Alert Name” field.
4. Type in an email address and click the “Add Email” button. This is the address of the person who will be notified when an alert is triggered. You can add multiple email addresses.
5. Select a Severity level (Low, Medium or High). This section is only enabled when the “Lockout” checkbox is selected. A “Low” selection will lock out the user by the categories monitored in the specific gauge only. A “Medium” selection will lock out the user from Internet access altogether. A “High” selection will lock out the users from all network protocols, so they cannot access the Internet, send e-mails, use instant messaging, or use P2P or FTP.

***NOTES**: Time-based lockouts can be set for a range of 30 minutes, one hour to eight hours, or unlimited.*

System Tray will not be shown in this demo, but if this feature is enabled, the administrator with an LDAP username, password and domain will see a system tray alert in the desktop system tray when an alert has been triggered. This applies to Active Directory environments only. For more information, please consult the Threat Analysis Reporter User Guide.

6. Create a Threshold per user. This numeric value is the number of times each user will be allowed to visit categories monitored by the gauge before triggering an alert.
7. Click on the “Submit” button to activate the alert.



Specify alert criteria

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 5: VIEW A URL TREND REPORT

TAR lets you generate historical trend reports that show activity by URL categories and bandwidth protocols for a specified time period. These trend reports are helpful for monitoring improvement of activity in a certain category as well as providing a good tool for setting appropriate thresholds for each TAR gauge.

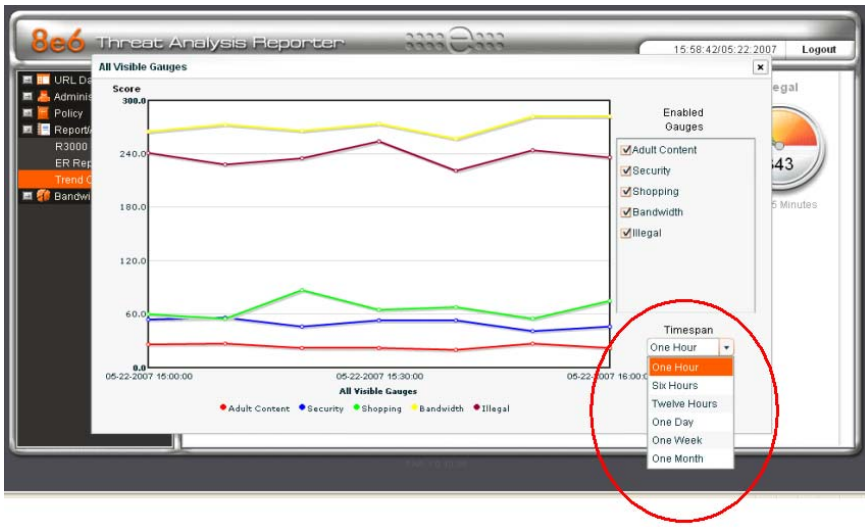
Step 1: Access Trend Charts

Click the “Report/Analysis” menu and then the “Trend Chart” sub-menu.

Select Trend Chart from left panel

Step 2: Change the Time Span

You can change the time span represented in the trend report by selecting one of five other options from the drop down menu. Choices range from the last hour to the last month of data.



View URL Trend Charts

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 6: MONITOR BANDWIDTH GAUGES

In addition to monitoring URL activity by user, TAR lets you view bandwidth activity by user, protocol and port for both inbound and outbound activity. This information can then be easily compared to the user's URL activity, providing a complete picture of the user's Web behavior.

Step 1: Select Bandwidth and Outbound

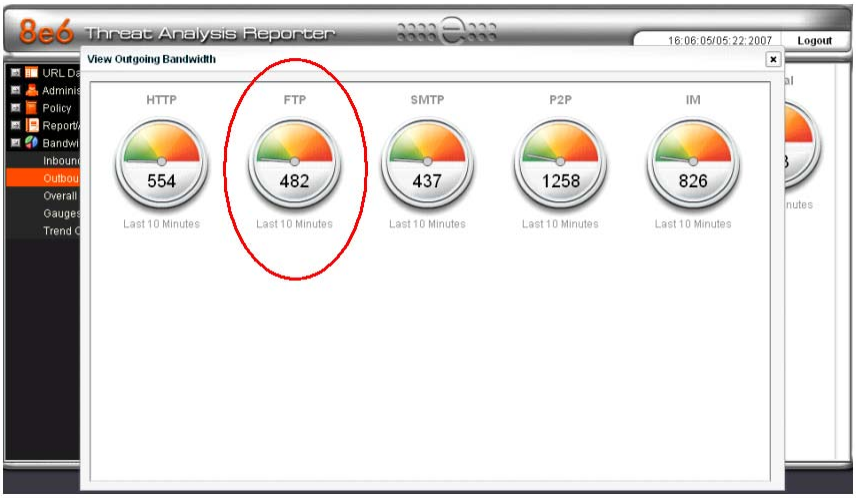
Select the "Bandwidth" menu option and the "Outbound" sub-menu option.

Select Bandwith and Outbound

Step 2: Select the FTP Protocol Gauge

Double-click the "FTP" protocol gauge.

***NOTE**: The "score" on bandwidth gauges is based on the number bytes of bandwidth consumed; not page hits, as with URL gauges.*

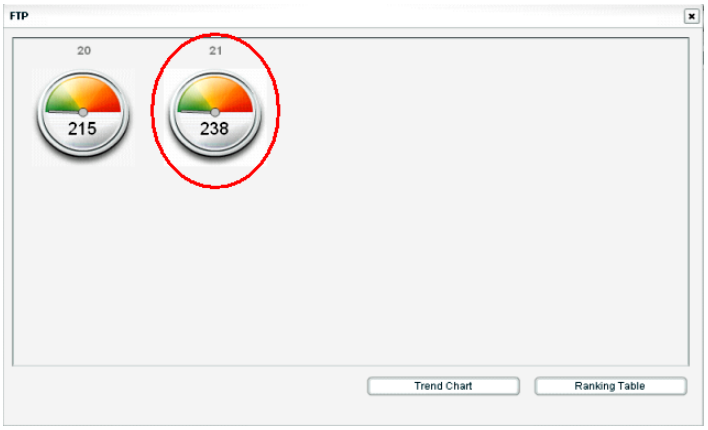


FTP gauge selected

Downloaded from www.Manualslib.com manuals search engine

Step 3: Select Port 21 Child Gauge

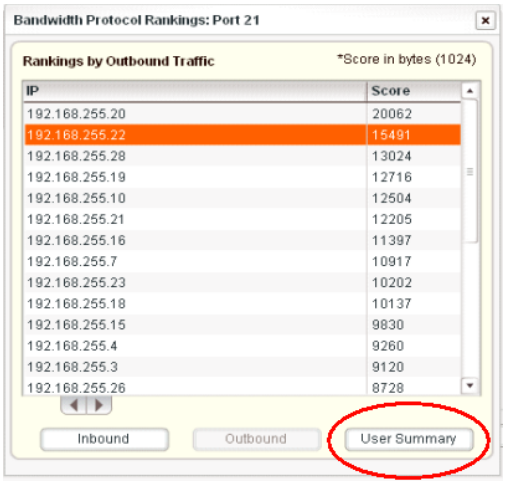
Double-click on “Port 21” child gauge.



FTP Port 21 gauge

Step 4: View the User Summary

Select one of the IP addresses in the list and then click the “User Summary” button.

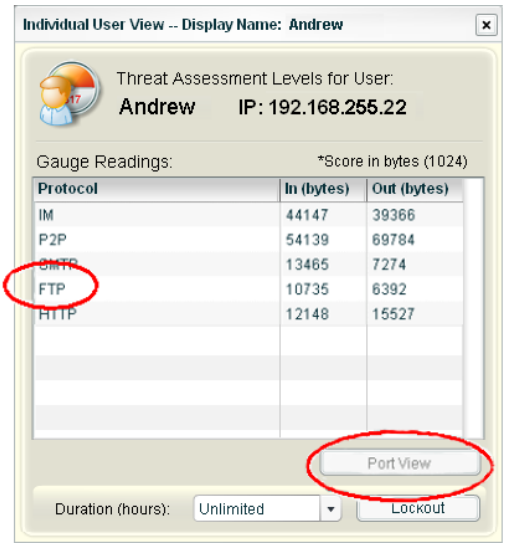


View User Summary

Downloaded from www.Manualslib.com manuals search engine

Step 5: View Port Traffic

Select the “FTP” protocol from the list and click the “Port View” button. The port traffic for this user will display for each of the ports assigned to FTP (e.g. Port 20 and 21).



View bandwidth used by end user

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 7: VIEW A BANDWIDTH TREND REPORT

As stated in Chapter 5, TAR has historical trend reports to demonstrate activity by URL categories and bandwidth protocols over a period of time. Bandwidth trend reports are helpful for monitoring bandwidth consumption improvement over time, as well as providing a good tool for setting appropriate thresholds for each TAR bandwidth gauge.

Step 1: Select Bandwidth and Trend Chart

Select the “Bandwidth” menu option in the left-hand menu and then select the sub-menu option “Trend Chart”. This action will open a pop-up window (see Step 2).

Bandwidth and Trend Chart selection

Step 2: View Bandwidth Trend Chart Data

You might try selecting multiple time spans in the same fashion as in the URL Trend Report. You may also de-select certain protocols by clicking the checkboxes in the “Enabled Protocols” window.

View Bandwidth Trend chart

Downloaded from www.Manualslib.com manuals search engine